Canada Border Services Agency | Agence des services frontaliers du Canada

Scenario-Based Targeting Governance Framework

Targeting Program,
Enforcement and Intelligence
Programs Directorate

Programs Branch

2018-03-15

PROTECTION • SERVICE • INTEGRITY

Canada

PREAMBLE

The CBSA Scenario-Based Targeting Governance Framework was drafted by the Targeting Program Unit within the Enforcement and Intelligence Programs Directorate, Programs Branch.

This document has been verified for technical accuracy at the time of publication and requests for additional use must be vetted through the Targeting Program Unit. This document may not be reproduced or distributed without the permission of the Targeting Program Unit. This publication is not intended for external use.

If access is requested under the *Access to Information Act* or *Privacy Act,* no decisions should be taken without prior consultations with the Targeting Program Unit, as the requested information may be subject to exemptions.

Table of Contents

Scenario-Based Targeting Governance Framework

Introduction

The Targeting Program identifies people and goods bound for Canada that may pose a threat to the security and safety of the country. The Canada Border Services Agency (CBSA) receives advance information from commercial air carriers to identify people for pre-arrival risk assessment purposes. The requirement for commercial air carriers to provide Advance Passenger Information (API) and all available Passenger Name Record (PNR) data, concerning all travellers (including crew) to the CBSA before a flight's departure, comes from section 5(a)-(f) of the Passenger Information Customs Regulations (PICR) and section 269(1)(a)-(f) of the Immigration Refugee Protection Regulations (IRPR). API and PNR enables the CBSA to identify in advance people who may pose a risk to national security, may be involved in illicit migration, or the smuggling of contraband. Domestic law and international agreements restrict Canada's use of PNR data to preventing and detecting terrorism offences or serious transnational crime while limiting the impact on privacy, civil liberties and human rights.

The API/PNR data is automatically screened through pre-determined Scenario-Based Targeting (SBT) rules known as scenarios within the CBSA Passenger Information System (PAXIS).. Scenarios are generated on the foundation of intelligence analysis of prior enforcement actions, trends and/or risk indicators that are associated to terrorism offences or serious transnational crime including contraband or illicit migration.

When API/PNR is received by the CBSA, it is processed through all active scenarios. If the traveller's information matches all criteria of a scenario, the traveller is placed on the "Scenario Work List" in PAXIS. Targeting Officers at the National Targeting Centre (NTC) will conduct comprehensive reviews on travellers who have matched scenarios in order to confirm or negate the potential risk. In addition to the scenario match, the traveller's information is processed through a number of queries to various internal and external databases either automatically or manually, in order to provide supplemental information for use during the review by the Targeting Officer. If the risk is determined to be valid, a target will be issued which will enable the interception of the traveller for further processing upon arrival in Canada.

Background

The CBSA committed to establishing a governance framework for the review of scenarios for effectiveness and proportionality and to ensure that the scenarios do not unnecessarily infringe upon the privacy, civil liberties or human rights of travellers.

CBSA Commitments

The CBSA adheres to all legislation and regulations with regard to the restrictions on the use of API and PNR, as defined in the *Protection of Passenger Information Regulations* (PPIR) and the *Passenger Information Customs Regulations* (PICR).

The consolidated requirements of the *PPIR, PICR,* and the strict program application guidelines can be found in the Directive Memorandum D1-16-3 *Guidelines for the Access to, Use, and Disclosure of Advance Passenger Information (API) and PNR Data*.

Civil Liberties & Human Rights

The program is responsible for ensuring each scenario component does not contain sensitive or personal data that may contravene the *Charter of Rights and Freedoms* or the *Canadian Human Rights Act*.

Civil liberties are the basic rights and freedoms granted to Canadian citizens as well as all foreign nationals on Canadian territory.

> Section 2 of the *Charter of Rights and Freedoms* guarantees everyone has the following fundamental freedoms: freedom of conscience and religion; freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication; freedom of peaceful assembly; and freedom of association.
>
> Section 15(1) of the *Charter of Rights and Freedoms* guarantees every individual is equal before and under the law and has the right to the equal protection and equal benefit of the law without discrimination and, in particular, without discrimination based on race, national or ethnic origin, colour, religion, sex, age or mental or physical disability.
>
> Section 3 of the *Canadian Human Rights Act* states that the prohibited grounds of discrimination are race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability and conviction for an offence for which a pardon has been granted or in respect of which a record suspension has been ordered.

In order to protect the civil liberties and human rights of travellers, the CBSA ensures that scenarios (including the trend analysis, API/PNR data elements, indicators, and scenario description derived from the trend analysis) do not contain any sensitive data as defined by the *Canada-European Union Passenger Name Record Agreement (CAN – EU PNR Agreement)*, which was developed having regard to the relevant provisions of the *Canadian Charter of Rights and Freedoms* and Canadian privacy legislation. Sensitive data is any information that could reveal:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Information about a person's health or sex life

A passenger's flight reservation may contain a Special Service Requirements (SSR) and/or a free text field which are part of the airline's Passenger Name Record (PNR) transmitted to the CBSA. As the SSR and/or free text field may contain "sensitive data", the CBSA's Data Acquisition Solution (DAS) purges these specific SSR data elements and those contained in the free text fields prior to displaying in PAXIS.

Minimal Privacy Intrusion

To minimize privacy intrusion, scenario descriptions or names cannot contain any information that may be considered sensitive data:

- meal preference (religious or philosophical beliefs / information about a person's health)
- family status (information about a person's sex life)
- disability requirements (information about a person's health)
- language (racial or ethnic origin)
- passport designation (political opinions)
- free text/information collected for analysis (applies to all sensitive data)
- birth city/country (racial or ethnic origin)

Scope of a Scenario

Scenarios are comprised of both API and PNR data elements. The use of PNR information is regulated by the PPIR; section 4(1) of the PPIR states:

> 4 (1) Subject to subsections (2) to (5), an official of the Agency may, for the following purposes, have access to any passenger name record information that is retained:
>
> (a) to identify persons who have or may have committed a terrorism offence or a serious transnational crime.
>
> (b) to conduct a trend analysis or develop risk indicators for the purpose referred to in paragraph (a).

API and PNR information will be used by the CBSA to target persons who will be subjected to closer questioning and/or examination upon arrival in Canada, or who require further investigation, for one of the purposes described above.

Meeting Regulatory Requirements: Terrorism Offences/Serious Transnational Crime

The Agency is permitted, as detailed in the *Protection of Passenger Information Regulations*, to use PNR for the purposes of identifying persons who have, or may have, committed terrorism offences or a serious transnational crime or to conduct trend analysis or develop risk indicators for the same purpose.

To meet regulatory requirements, each scenario must include the specific statutory authority (i.e., *Customs Act*, *Immigration and Refugee Protection Act*) that supports the creation of the scenario;

and, include a brief summary as to how the scenario meets the requirements. This information must always be included with the scenario to ensure throughout the life of the scenario there is always a link to the statute, legislation and regulation that supports it.

The scenario must focus on identifying individuals who have or may have committed a terrorism offence or serious transnational crime. The trend analysis, the PNR data elements, the indicators and the scenario description must be developed in accordance with the regulations and reflect the allowable purpose, for which it is created.

A scenario meets the regulatory requirements under the following conditions:

- the initial purpose of developing the scenario is supported by the regulations;
- the scope and use of the scenario is supported by the regulations; and
- each scenario is specifically developed for identifying terrorism offences or serious transnational crime.

Terrorism offence is defined in the PPIR as follows:

> Terrorism offence means
>
> (a) an act or omission that is committed for a political, religious or ideological purpose, objective or cause with the intention of intimidating the public with regard to its security, including its economic security, or with the intention of compelling a person, government or domestic or international organization to do or refrain from doing any act, and that is committed with the intention to
>
> - (i) cause death or serious bodily harm,
> - (ii) endanger a person's life,
> - (iii) cause a serious risk to the health or safety of the public,
> - (iv) cause substantial property damage that is likely to result in the harm referred to in any of subparagraphs (i) to (iii), or
> - (v) cause serious interference with or serious disruption of an essential service, facility or system other than as a result of lawful or unlawful advocacy, protest, dissent or stoppage of work, such as a strike, that is not intended to result in the harm referred to in any of subparagraphs (i) to (iii);
>
> (b) an act or omission referred to in paragraph (a) of the definition terrorist activity in subsection 83.01(1) of the Criminal Code;
>
> (c) knowingly participating in or contributing to an activity for the purpose of enhancing a terrorist group's ability to facilitate or commit an act or omission referred to in paragraph (a) or (b) or instructing a person, group or organization to carry out an activity for that purpose;
>
> (d) an indictable offence if the act or omission that constitutes the offence is committed for the benefit of, at the direction of or in association with a terrorist group;

(e) any of the following, if they are carried out for the purpose of committing an act or omission referred to in paragraph (a) or (b):

- (i) collecting, using or possessing property,
- (ii) providing or making available property or a financial or related service, or
- (iii) inviting a person, group or organization to provide property or a financial or related service;

(f) attempting or threatening to commit an act or omission referred to in paragraph (a) or (b);

(g) conspiring to commit, or facilitating, instructing or counselling the commission of, an act or omission referred to in paragraph (a) or (b);

(h) being an accessory after the fact to an act or omission referred to in paragraph (a) or (b); or

(i) harbouring or concealing for the purpose of enabling a terrorist group to facilitate or commit an act or omission referred to in paragraph (a) or (b). (terrorism offence)

Serious transnational crime is defined in the PPIR as follows:

> Serious transnational crime means an act or omission that constitutes an offence punishable in Canada by a maximum term of imprisonment of at least four years and that is committed
>
> (a) in more than one country;
>
> (b) in only one country but a substantial part of its preparation, planning, direction or control takes place in another country;
>
> (c) in only one country but an organized criminal group that engages in criminal activities in more than one country is implicated in the act or omission;
>
> (d) in only one country but has substantial effects in another country; or
>
> (e) in a country other than Canada but the offender intends to travel to or transit through Canada. (crime transnational grave)

Examples of serious transnational crime are included in paragraph 15 of Departmental Memorandum D1-16-3, *Guidelines for the Access to, Use, and Disclosure of Advance Passenger Information (API) and Passenger Name Record (PNR) Data*:

> 15. Examples of serious transnational crimes include, but are not limited to:
> (a) narcotics smuggling;
> (b) human smuggling;
> (c) human trafficking; and
> (d) importation or smuggling of child pornography.

Scenario Risk Categories & Legislative Authorities

The *Customs Act and* the *Immigration and Refugee Protection Act* (IRPA) are the primary legislative authorities that allow the CBSA to identify risks for National Security, Contraband and Illicit Migration.

A) National Security Scenarios:

i) National Security – Canadian Citizens (*Canada Border Services Act*, Sections 2 and 5)

The examination of Canadian Citizens for national security is limited to statutory provisions contained in the CBSA program legislation, as defined in section 2 of the CBSA Act, and the mandate of the Agency as established in section 5 of the CBSA Act.

ii) National Security – Goods (*Customs Act*, S. 159)

The legislative authority to risk assess, identify and intercept goods associated to national security risks is found in Section 159 of the *Customs Act*. National Security scenarios are developed using intelligence information, trend and threat analysis associated to the transportation of prohibited goods identified as terrorism propaganda (D9-1-18).

iii) Security – Foreign Nationals or Permanent Residents (IRPA Section 34 (1) (a – f))

National security scenarios identifying risks to 'Security' are designed using intelligence information and/or trend analysis that identifies foreign nationals or permanent residents who have or may have committed a terrorist offence and may be inadmissible under the IRPA Section 34 for those reasons.

B) Contraband Scenarios (*Customs Act*, S. 159):

The legislative authority to intercept contraband risks is Section 159 of the *Customs Act*. Contraband scenarios must be designed using previous enforcement actions/intelligence or partner information that identifies individuals who have or may have committed a serious transnational crime.

C) Illicit Migration Scenarios:

i) Human or International Rights Violations (IRPA Section 35 (1) (a – c))

Illicit migration scenarios identifying risks to 'Human or International Rights Violations' must be designed using analysis of previous enforcement actions/intelligence or partner information that identifies foreign nationals or permanent residents, who may have committed human or international rights violations, and, who have or may have committed a terrorist offence or a serious transnational crime and, may be inadmissible under the IRPA Section 35 for those reasons.

ii) Serious Criminality (IRPA Section 36 (1) (a – c) Section 36 (2) (a –c))

Illicit migration scenarios identifying risks to 'Serious Criminality' must be designed using analysis of previous enforcement actions/intelligence or partner information that identifies foreign nationals or permanent residents who have or may have committed a serious transnational crime and may be inadmissible under the IRPA Section 36 for those reasons.

iii) Organized Criminality (IRPA Section 37 (1) (a) (b))

Illicit migration scenarios identifying risks to 'Organized Criminality' must be designed using analysis of previous enforcement actions/intelligence or partner information that identifies foreign nationals or permanent residents who may belong or have belonged to an organized criminal group, who are known to have or may have committed a serious transnational crime and may be inadmissible under the IRPA Section 37 for those reasons.

iv) Human Smuggling (IRPA Section 117)

Illicit migration scenarios identifying 'human smuggling' risks must be designed using intelligence analysis that identifies foreign nationals who may be involved in illicit migration through the organized transport of a person across an international border (clandestine smuggling or fraudulent activities). The legislative authority related to human smuggling is included in section 117 of IRPA.

Illicit migration scenarios must focus on those that have or may have committed an offence linked to human smuggling; and/or, those that demonstrate, through act or omission knowledge or linkages to individuals or criminal groups that have or may have committed serious transnational crimes i.e. human smuggling.

v) Human Trafficking (IRPA Section 118)

Illicit migration scenarios identifying 'human trafficking' risks must be designed using intelligence analysis that identifies foreign nationals and/or Canadians who may be victims, or organizers of human trafficking related activities. The legislative authority related to human trafficking is included in section 118 of IRPA as well as multiple other legislative authorities found in the *Criminal Code of Canada*. The various laws application can respond to trafficking including kidnapping, forcible confinement, aggravated sexual assault, extortion, organized crime and prostitution-related offences.

Illicit migration scenarios must focus on those that have or may have committed an offence linked to human trafficking; and/or, those that demonstrate, through act or omission knowledge or linkages to individuals or criminal groups that have or may have committed serious transnational crimes i.e. human trafficking.

Scenario Creation and Review

SBT rules undergo various levels of review throughout their development and maintenance. Scenarios are developed based on information from a variety of sources, which include recent significant interdictions that are cross-referenced with historical enforcement and intelligence information, as well as with API/PNR information for interdicted subjects, information from Liaison Officers overseas, international intelligence bulletins, port of entry seizures, CBSA

intelligence bulletins, and actionable indicators and trends from partner agencies based on their area of expertise.

The NTC Targeting Intelligence (TI) unit is responsible for analyzing the types of information that contribute to scenarios,

All SBT rule proposals identify the supporting information and source that justifies the rationale and intelligence behind its development.

The National Targeting Centre (TI, TT and TRIS) all review and track each step in the scenario development process including activations and modifications to ensure that prior to activation, scenarios meet CBSA policies and procedures including API/PNR legislative and regulatory use requirements, and do not have a negative impact on privacy, human rights and civil liberties.

Prior to activation, the scenario is impacted for volumetrics through the Targeting Data Analytics (TDA) unit and reviewed by Targeting Travellers (TT) for operational impacts and implementation with the objective to minimize traveller impacts. The Targeting Program Unit (TPU) will be provided with the scenario at the same time as TT and will conduct a review (Appendix A: Scenario Review Process), without impeding the scenario activation process, to ensure adherence to the appropriate statutory/regulatory requirements. If it is determined that a scenario possibly infringes upon the civil liberties, privacy or human rights of a traveller, TI will be immediately notified to discuss resolution. A communication protocol is further outlined in Appendix A.

The proposal is reviewed by the Targeting Rules, Indicators and Scenarios (TRIS) unit to ensure the scenario can be coded and activated in PAXIS. Once a scenario is activated, TRIS utilizes a rigorous monitoring and maintenance framework through which performance is reviewed and documented.

SBT Governance

The governance surrounding SBT leverages the existing targeting organizational framework to ensure it is effectively and efficiently managed and complies with international agreements, legislative and regulatory requirements.

Scenario Management Committee (SMC)

This Committee is responsible for making recommendations by conducting ongoing reviews of scenarios, scenario development, and management procedures to ensure scenario effectiveness, procedural efficiency, consistency and integrity. Scenarios viewed as ineffective, or not fulfilling program requirements may be deactivated or modified, and procedures will be

updated as required. In addition, the Committee investigates and reports on issues that impact the SBT process. The SMC is also responsible for reporting to the TPMC.

For further information, refer to the Terms of Reference (TR) of the SMC (Appendix B).

Targeting Program Management Committee (TPMC)

The mandate of this Committee is to ensure the management of the Targeting Program, including SBT, is efficient and effective, as well as operationally compliant with international agreements, legislative and regulatory requirements. In order to achieve this, the TPMC leverages the existing organizational framework and ensures the necessary leadership, communication and processes are in place.

For further information, refer to the TR of the TPMC (Appendix C).

Roles and Accountabilities

Operations Branch, National Border Operations Centre (NBOC), NTC

The NTC is responsible for the operational development and delivery of SBT, thereby making it accountable for the following:

- Ensuring adherence to all legislative, regulatory and policy requirements including written collaborative agreements, treaties and memoranda of understanding;
- Evaluating each scenario prior to activation to ensure compliance with all privacy, legislative and regulatory requirements;
- Developing and maintaining SBT operational procedures including scenario development, activation, monitoring and deactivation;
- Analyzing intelligence, reviewing examination and enforcement results, including the risk environment, trends and patterns to develop, modify or deactivate scenarios;
- Ensuring scenarios are operationally manageable and proportionate by assessing the operational impacts prior to activation;
- Collaborating with stakeholders in the scenario creation process;
- Recording and storing all intelligence and information used to develop a scenario in addition to maintaining the scenario development tracking log and scenario master list;
- Retaining all targeting scenario proposal templates in addition to recording the activation, modification and deactivation of scenarios;
- Identifying and monitoring API/PNR data quality and consulting with internal partners regarding data provision issues that impact the effectiveness of scenarios or the efficiency of PAXIS;
- Developing and distributing SBT performance reports to internal stakeholders;

- Assuming the responsibility for the scenario lifecycle including scenario development, activation, modification, and deactivation;
- Utilizing and maintaining a detailed log to provide an auditable record of scenario legislative and regulatory compliance review; and
- Coordinating meetings and maintaining records of the SMC.

Programs Branch, Enforcement and Intelligence Programs Directorate, Targeting Program Unit

The Targeting Program Unit is the functional authority for the targeting program, and is responsible for providing program strategy and policy direction related to SBT. Its accountabilities include:

- Providing strategic and functional direction to Operations Branch, and program policy, privacy, legislative and regulatory guidance to senior management concerning scenario-based targeting;
- Maintaining the *Scenario-Based Targeting Governance Framework*;
- Evaluating each scenario prior to activation to ensure compliance with all privacy, legislative and regulatory requirements (for more information, refer to Appendix A "Scenario Review Process");
- Coordinating meetings and maintaining records of the Targeting Program Management Committee;
- Discussing SBT related issues with the Operations Branch, NBOC;
- Reporting and escalating issues on SBT-related matters, including program and policy matters and systems issues as required; and
- Supporting the NTC to evaluate systems, tools, business and process improvements facilitating operational delivery and ongoing enhancement of SBT (i.e. new systems/applications, analytical tools systems improvements and processes – e.g. PAXIS, SPSS modeller, and data warehouse).

Programs Branch, Traveller Programs Directorate, Air Programs Unit

The Air Programs Unit develops, amends, and maintains legislation and regulations related to traveller processing in the air mode and is the Office of Primary Interest for the API/PNR Program and PAXIS. Its accountabilities include:

- Providing program strategy and policy direction related to the collection and use of API/PNR;

- Developing and maintaining related high-level policies, regulations, and legislation for the acquisition and use of API and PNR data;
- Controlling and approving requests for access to PAXIS;
- Coordinating targeting and API/PNR systems changes/fixes or projects in conjunction with the Business Systems Integration Division; and
- Co-chairing (with the Targeting Program unit) the API/PNR Program and Targeting Program bi-weekly meetings where issues related to the API/PNR and Targeting Programs are identified, discussed, tracked and resolved.

Issue Escalation Process

1. Issues are first discussed between the Programs and Operations Branches' subject matter experts (SMEs).
2. If initial concerns raised between the SMEs are not resolved, the issue(s) are then brought to the SMC for a collective discussion and dispute resolution.
3. If the initial concerns that were raised during the SMC meeting are not resolved, the issue(s) are raised to the TPMC
4. If the initial concerns raised at TPMC are not resolved, the issue(s) are raised to the Enforcement and Intelligence Program Management Table (E&I PMT), the Traveller PMT or both, as required.

Note: any discussion between Programs and Operations on specific scenario issues are to be retained in the Operations' scenario folder.

The Chair and Deputy Chair of the E&I PMT (see Appendix D for the Terms of Reference) are accountable for providing guidance and direction to the responsible Directors as follows:

- Ensuring strategic planning and horizontal communications with regards to SBT.
- Providing guidance on implementing and monitoring performance measures.
- Identifying and leveraging best practices for SBT.
- Reviewing program costs and identifying opportunities for savings within SBT.
- Ensuring overall alignment with Agency priorities or long-term planning.

Appendix A: Scenario Review Process

Introduction

During the development of a scenario, the Canada Border Services Agency (CBSA) ensures that it does not contain any sensitive data, intrude on privacy, or violate civil liberties and human rights. The Agency will review each scenario prior to activation or modification in order to identify any potential impacts and to ensure compliance with current policy, legislation and regulations.

This appendix outlines the scenario components that are included in the review as well as the communication protocol for the National Targeting Centre (NTC) Operations and the Targeting Program authority.

Scenario Components

The National Targeting Centre (TI, TT and TRIS) review and track each step in the scenario development process including activations and modifications to ensure that prior to activation, scenarios meet CBSA policies and procedures including API/PNR legislative and regulatory use requirements, and do not have a negative impact on privacy, human rights and civil liberties.

The Targeting Program unit (TPU) is responsible for the review of the scenario components prior to the activation or modification of a scenario to ensure adherence to CBSA policy, statutory and regulatory requirements.

The following scenario components will be reviewed by TPU:

1. Scenario Template
2. Scenario Description

1) Scenario Template

The scenario template must encompass the appropriate statutory requirements according to the applicable risk.

The *Customs Act* and *IRPA* are the primary legislative authorities that allow the CBSA to identify risks for the three categories of Contraband, Illicit Migration and National Security.

- Ensure the appropriate legislative authority (i.e. *Customs Act* or *IRPA)*, accurately reflects the identified risk category for terrorism or serious transnational crime.

2) Scenario Description

The scenario description includes the results of the trend analysis to support the scenario and the specific risk(s) for terrorism offences or serious transnational crimes meant to be captured by the scenario.

- Ensure the scenario description meets the regulatory requirements by not infringing on a person's privacy, civil liberties and human rights.

Communication Protocol

Following the intelligence analysis to develop the scenario and upon receipt of the operational volume impacts, Targeting Intelligence provides the draft scenario template to TT and TPU.

TT will review the draft scenario template for operational impacts and will advise TI upon approval.

TPU will review the draft scenario template, without impeding the scenario activation process, to ensure adherence to the appropriate statutory/regulatory requirements. If the scenario template and/or description does not meet the appropriate statutory/regulatory requirements, TPU will contact TI for further consultation.

TI provides TRIS with the TT-approved scenario template for activation. Once the scenario elements and description have been finalized, TRIS will provide TPU with the finalized version of the scenario template just prior to activation.

If the scenario template and/or description does not meet the appropriate statutory/regulatory requirements, TPU will contact TI and TRIS for further consultation to either deactivate or modify the scenario.

Should there be differing interpretations of the statutory/regulatory requirements, the concern will be raised at the next monthly Scenario Management Committee for resolution. If not resolved, the issue escalation process will be followed as detailed in the body of this framework document.

Appendix B: Terms of Reference – Scenario Management Committee

Context/Background

Scenario-Based Targeting (SBT) is a key part of the Canada Border Services Agency's (CBSA) pre-arrival traveller targeting program and supports the Agency's Risk Assessment Program by contributing to the identification and interception of suspected potential high and unknown risk people that may pose a threat to the national security, safety and prosperity of Canada. It also fulfils a commitment made by the CBSA under the Beyond the Border Action Plan to implement an enhanced SBT targeting methodology similar to that of the United States Customs and Border Protection.

Increasing targeting work volumes, finite resources, ongoing scrutiny of standardized/automated risk assessment and border security approaches and ever-changing risks/threats, necessitate ongoing robust rigour and scrutiny of the CBSA's risk management and assessment tools such as pre-arrival targeting's SBT process. In order to ensure the integrity and effectiveness of SBT and the overall success of the CBSA's traveller targeting program, the effectiveness of scenarios and the efficiency and integrity of their development and management processes/procedures, needs to be regularly reviewed and adjustments made as required.

Mandate/Expected Outcome

To ensure scenario based targeting is effective and complies with privacy, legislative and regulatory requirements.

Membership

Chair: NTC TRIS Manager
Co-Chair: NTC TI Manager
Secretariat: Targeting Rules Indicators and Scenarios (TRIS)

Representatives

- NTC – Targeting Intelligence (TI)
- NTC – Targeting Traveller (TT)
- NTC – Targeting Rules, Indicators and Scenarios (TRIS)
- NTC – Targeting Data Analytics (TDA)
- Targeting Program Unit
- Air Programs

* Note[1]: Other areas may be invited to attend meetings on an ad-hoc basis dependent upon specific agenda items.

* Note[2]: Members require Secret clearance and a working knowledge of SBT.

Meeting Frequency

Monthly

Members Roles and Responsibilities

- identify and discuss issues impacting scenarios (ex: data quality provision, review rates, scenario capacity limit, and elements for coding);
- provide recommendations for resolution;
- request additional information from Subject Matter Experts on scenarios;
- discuss and recommend scenarios for a possible scenario effectiveness assessment (SEA);
- review the outcome of the SEA; and
- Receive timely updates of legislative, regulatory, initiatives, systems, international or national agreements impacting SBT from Program authority.
- Review and make amendments to scenario development and processes and procedures, as required;
- Raising of issues to the Targeting Program Management Committee (TPMC) in accordance with the issues escalation process.

Meeting Organization

- A program officer from TRIS will act as the committee secretariat.
- Working group meetings will be held once a month; may be held more often as required.
- A report on the month's scenario activations, modifications and deactivations will be prepared by TRIS for discussion at the meeting.
- Records of discussion will be drafted and shared by the committee secretariat.

Appendix C: Terms of Reference – Targeting Program Management Committee

Mandate

To ensure the management of the Targeting Program is efficient and effective, as well as operationally compliant with international agreements, legislative and regulatory requirements. In order to achieve this, the Targeting Program Management Committee (TPMC) will leverage the existing organizational framework and will strive to have the necessary leadership, communications and processes in place.

Membership

Chairs:
Director of Intelligence, Targeting and Criminal Investigations Programs Management Division and

Director of the National Targeting Centre

Note: The Director of Program Compliance and Outreach, Commercial Programs, will be an additional co-chair for TPMC-commercial meetings only

Secretary:
Targeting Program Unit

Members:
To include Managers and/or their representatives from the following areas:
Operations Branch:

- Commercial Operations Division
- National Targeting Centre
- Intelligence Operations and Analysis Division
- Traveller Operations Division

Programs Branch:

- Commercial Program and Policy Management Division
- Intelligence, Targeting and Criminal Investigations Programs Management Division
- Traveller Program and Policy Management Division

Note: Other areas may be invited to attend meetings on an ad-hoc basis dependent upon specific agenda items (i.e. IT or BSID).

Authority

The co-chairs of the committee have the authority to set the overall strategic direction of the Committee, to approve Committee agendas, and to request items be brought forward at a specified date.

The co-chairs retain the decision-making authority as to when to escalate items put before the committee if consensus cannot be achieved; however, the co-chairs shall seek to build consensus among members in carrying out this duty.

Roles and Responsibilities

To fulfill its mandate, the committee will:

- Receive a briefing from the Scenario Management Committee (SMC) meetings (for TPMC-traveller meetings only).
- Receive a briefing from the Commercial Risk Capability Management Committee (CRCMC) Committee meetings (for TPMC-commercial meetings only).
- Review and discuss targeting performance measurement, budget planning and accountability requirements.
- Identify and discuss data quality issues and industry data submission compliance rates.
- Identify and discuss effectiveness of national and regional intelligence in support of the National Targeting Model.
- Develop, review or recommend targeting policy, procedures, guidelines, processes and system requirements.
- Identify, analyze and propose solutions for any issues that have an impact on the delivery of the Targeting Program such as system issues and limitations, human resource planning, recruitment processes and training.
- Identify, analyze and propose solutions for any issues that have a direct impact on the success of the Targeting Program, such as the essential "inputs" (National, Regional, Internal Intelligence, data (internal, external), Exam Results (closing the loop), Partnerships (GC, International), as identified in the Internal Audit and Program Evaluation.

Meeting Frequency:

Separate committees will be held for commercial and travellers streams each month. It is anticipated there will be a joint commercial-travellers TPMC held two times a year to discuss cross-cutting issues in a consolidated forum.

Record of Discussion and Decision:

The secretariat of the committee is responsible for drafting and disseminating a Record of Discussion and Decision (RDD) to all attendees after a meeting is held.

Escalation:

The co-chairs are responsible for escalating, to the appropriate parties, any issues emanating from the meeting after an issue is identified.

Proxies to meetings:

Members of the committee shall nominate a proxy to attend a meeting if the member is unable to attend. Proxies are expected to brief all affected parties within their Unit, Division and Directorate on all decisions made at the committee.

Please note that membership is recommended to be at the manager and senior advisor level. Proxies should be first at the senior advisor level and if neither the manager nor senior advisor is available, a senior program officer can represent their area.

Quorum Requirements:

A minimum of four (4) committee members is required for the meeting to be recognized as an authorized meeting. If either of the co-chairs or their representatives is unavailable, the scheduled meeting may be cancelled or rescheduled.

Appendix D: Terms of Reference – Enforcement and Intelligence Program Management Table

Mandate

The Enforcement and Intelligence Program Management Table (EI PMT) members will consult jointly and provide integrated and functional guidance to the following eight (8) EI programs: Intelligence, Targeting, Security Screening, Criminal Investigations, Immigration Investigations, Detentions, Hearings and Removals. The Intelligence Program also includes some areas under International Region and the National Targeting Centre.

This PMT is a focussed, action-oriented decision making body and is responsible for providing leadership on the EI's program strategic policy direction, priority setting, performance measurement, risk identification and mitigation strategies, workforce training and leaning requirements and making financial recommendations.

Membership

Chair	• Director General, Enforcement and Intelligence Programs Directorate, Programs Branch
Deputy Chair	• Director General, Enforcement and Intelligence Operations Directorate, Operations Branch
Secretariat	• Director, Program Performance, Reporting and Transformation Division, Enforcement and Intelligence Programs Directorate, Programs Branch
Standing Members	• Executive Director, Enforcement & Intelligence Programs, Programs Branch • Director General, Global Border Management and Data Analytics, Programs Branch • Director General, International Operations, Operations Branch • Executive Director, Pacific Region, Operations Branch • Director General, Training & Learning, Human Resources Branch • Director General, Corporate Governance & Accountability, Corporate Affairs Branch • Director General, Resource Management Directorate, Comptrollership Branch • Director, National Targeting Centre, Operations Branch • Director General, Transformation and Oversight, Comptrollership Branch • Director General, Enterprise Architecture/Information Management, IST Branch

	• Directors, Enforcement and Intelligence Programs, Programs Branch • Senior Advisor, Programs & Operations Communications, Communications Directorate, Corporate Affairs Branch
Ad Hoc Members	• Directors, Enforcement and Intelligence Operations, Operations Branch ****Based on the agenda items, attendance to the PMT will vary for Ad Hoc Members****

Note: Each Standing Member of the EI PMT shall nominate one proxy at the Director level to attend meetings in the event that the Member is unable to attend. Every effort should be made by each Standing Member to attend all meetings. Every effort should also be made to ensure that a proxy is available for all meetings that the Standing Member is unable to attend, and is well briefed on the operations of the PMT. Subject matter experts and observers may be invited to attend a PMT meeting at the Chair's discretion.

Responsibilities and Duties

The EI PMT has the responsibility for decisions that affect the functional direction and oversight, budget management, and monitoring and performance reporting of the Enforcement and Intelligence Programs. To do this, the EI PMT will focus on the following areas:

1. Serve as an active and dynamic oversight body with regards to financial, budgetary, training and learning, and human resources planning issues, and provide input on the PMT's forward agenda.

2. Support vertical and horizontal communications and engagements and seek to build consensus among Standing Members and Ad Hoc Members.

3. Provide strategic direction for EI stakeholder engagement, including (a) form and dissolve EI level committees, and (b) establish reporting requirements for committees. These committees will then analyze/examine and propose resolutions and report back their findings to the EI PMT.

4. Ensure alignment of identified priorities and evaluate performance measurements on a quarterly basis.

5. Report to the President on the PMT progress on established performance indicators and make recommendations relating to Criminal Investigations, Immigration Enforcement Program Activities and Targeting, and the Intelligence and Security Screening Program Sub-Activities, in collaboration with the Program Policy Committee (PPC) and Executive Committee (EC).

6. Provide direction to the PMT Secretariat for all corporate and logistical matters to ensure effective and efficient PMT meetings.

Chair

The duties of the Chair of the EI PMT are an extension of his or her organizational responsibilities as the DG of the Enforcement and Intelligence Programs Directorate.

1. Serve as the single point of accountability for the PMT, as well as the decision-making authority on items put before the PMT.

2. Retain the sole authority to make a decision to escalate issues to the Program Policy Committee (PPC) for consideration, resolution, and/or guidance.

3. Responsible for vertical and horizontal communications and engagement.

4. Establish a results measurement framework for monitoring the PMT's performance, while evaluating progress on a quarterly and annual basis.

5. Facilitate meaningful and effective meetings, ensuring that items brought to the PMT have been broadly and adequately consulted.

6. Determine PMT membership in collaboration with the Deputy Chair.

7. Responsible for providing direction to the PMT Secretariat for all corporate and logistical matters to ensure effective and efficient PMT meetings.

8. Delegate duties and oversight of certain areas of responsibility to the Deputy Chair.

Deputy Chair

1. Assume the roles and responsibilities of the Chair in the Chair's absence, as well as other duties and responsibilities as assigned by the Chair.

2. Collaborate with the Chair in determining PMT membership.

3. Build consensus with the Chair, on key issues and decision points before and after PMT meetings, to address contentious issues, potential conflicts of interest and work towards integrating program and operational activities to achieve the best results possible.

4. Consult with senior management in the Regions and represent their views to the extent possible at EI PMT meetings, while reporting back to them on all PMT business.

Governance Structure

The EI PMT is accountable to the Program Policy Committee (PPC). The role of the PPC is to advise Executive Committee (EC) on strategic policy and ensure the ongoing development of CBSA policy and program delivery and to identify and manage functional management issues in relation to risk.

The PMT is the governing authority for director-level committees and managerial program committees. Director level committees are:

- National Inland Enforcement Committee,
- National Intelligence, Targeting and Security Screening Committees, and
- National Criminal Investigations Committee.

Committee membership is composed of both Headquarters and regional members.

Managerial working level groups should exist for all EI Programs. Managerial level working group membership is composed of the program's respective national managers and regional managers.

It is expected that issues will be brought forward at the appropriate working level and follow the governance hierarchy in seeking approvals by, or providing briefings to, the relevant decision-making body. Director level committees may additionally wish to seek approval or consult with the EIOD Directors/DG Operations Committee on relevant issues.

The committees and working groups meet on a regularly scheduled basis and report to the PMT quarterly on issues such as risk/risk mitigation, performance and financial management.

Please see the Annex for further details on the EI PMT Governance structure.

Table Operation

Frequency and Duration

The EI PMT shall meet on a three week schedule on Wednesdays, or more frequently if required. *Ad hoc* meetings may be scheduled as required at the request of the Chair.

Quorum

A minimum of four EI PMT Standing Members, including the Chair or the Deputy Chair, are required for the meeting to be recognized as an authorized meeting.

Materials and Records of Discussion

The EI PMT Secretariat will prepare the Agenda and the Record of Discussion (RoD) for each meeting and provide to the Chair for final review and approval. The RoD shall include clear action items, with assigned leads and Brought Forward (BF) dates. It will also include standing and forward agenda items. The Secretariat is responsible for disseminating the RoD to all Standing Members prior to the next meeting. RoDs and Annexes will be made available to EI PMT Members as needed in an effort to promote information sharing. The RoD and identified action items from each meeting will be maintained and monitored by the Secretariat.

The Chair shall finalize and approve the agenda for each EI PMT meeting one week before the scheduled meeting. Materials are normally available to EI PMT Members two business days in advance of any meetings.

Values Based Leadership and Organizational Culture

EI PMT Members, through their actions and words, shall demonstrate their commitment to the highest standards of integrity, ethical values and professionalism in the performance and functional management of programs.

Annex: